data generating code for generating data for an image;

first encrypting code for encrypting the data using a first key;

second encrypting code for twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

generating code for generating a header containing the twice-encrypted first key;

first transmitting code for transmitting the header to the intended image output device;

receiving code for receiving a request from the intended image output device for the encrypted data; and

second transmitting code for transmitting the encrypted data to the intended image output device.

123. A printer driver according to Claim 122, wherein the first transmitting code transmits the header to the intended image output device by e-mail.

- 2 -

124. A printer driver according to Claim 122, wherein the header which is generated in the generating code also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

125. Computer-executable process steps stored on a computer-readable medium, the computer-executable process steps for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, said computer-executable process steps comprising:

receiving code to receive twice-encrypted data;

decrypting code to twice decrypt the twice-encrypted data using a first key and a second key, the first key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the second key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; and

an image generating code to generate an image from the decrypted data.

126.   Computer-executable process steps stored on a computer-readable medium, the computer-executable process steps for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, said computer-executable process steps comprising:

receiving code to receive encrypted data and a twice-encrypted first key;

first decrypting code to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;

second decrypting code to decrypt the encrypted data using the decrypted first key; and

image generating code to generate an image from the decrypted data.

127.   Computer-executable process steps according to Claim 126, wherein the first decrypting code utilizes an asymmetric decryption algorithm.

- 4 -

128. Computer-executable process steps according to Claim 126, wherein the second decrypting code utilizes a symmetric decryption algorithm.

129. Computer-executable process steps according to Claim 126, wherein the first decrypting code decrypts the twice-encrypted first key using the second key before decrypting the twice-encrypted first key using the third key.

130. Computer-executable process steps according to Claim 126, wherein the first decrypting code decrypts the twice-encrypted first key using the third key before decrypting the twice-encrypted first key using the second key.

131. Computer-executable process steps according to Claim 126, wherein the third key is contained within the intended image output device, whereby the third key is primarily shielded from access by devices other than the intended image output device.

132. Computer-executable process steps according to Claim 126, wherein the second key is contained in a smart-card possessed by the intended recipient, whereby the second key is hidden from recipients other than the intended recipient.

133. Computer-executable process steps according to Claim 126, wherein the receiving code further receives a signed header hash and a signed data hash, the method further comprising verifying code to verify the authenticity and the integrity of the signed header hash and of the signed data hash.

134. Computer-executable process steps according to Claim 133, further comprising code to discard the encrypted data rather than outputting an image based upon the encrypted data, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

135. Computer-executable process steps according to Claim 134, further comprising code to send a notice to a sender of the signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

136. Computer-executable process steps according to Claim 126, wherein the intended image output device is a printer.

137. Computer-executable process steps according to Claim 126, wherein the intended image output device is a facsimile machine.

138. Computer-executable process steps stored on a computer-readable medium, the computer-executable process steps for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

receiving code to receive a header containing a twice-encrypted first key;

sending code to send a request for encrypted data corresponding to the header;

receiving code to receive encrypted data corresponding to the header;

first decrypting code to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;

second decrypting code to decrypt the encrypted data using the decrypted first key; and

image generating code to generate an image from the decrypted data.